U.S. DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
FILED
MAR 23 2017
CLERK, U.S. DISTRICT COURT
By Deputy

UNITED STATES DISTRICT COURT

for the
Northern District of Texas

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Black Alcatel One Touch cellular telephone, model A564C, SN: 535D315E and an RCA tablet with pink backing with charge cord, SN: P3EH1Z1353D5

Case No. 4:17-MJ-261

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A.

located in the Northern District of Texas, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. § 2252 and 2252A	Transportation, receipt, possession, and distribution of child pornography

The application is based on these facts:

See attached Affidavit.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: __________) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Stephanie Phillips, FBI Task Force Officer
Printed name and title

Sworn to before me and signed in my presence.

Date: 3/23/17

Judge's signature

City and state: Fort Worth, Texas

Jeffrey L. Cureton, United States Magistrate Judge
Printed name and title

AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

Affiant, Stephanie Phillips, being duly sworn states as follows:

I am submitting this affidavit in support of an application for a search warrant authorizing the search of two devices: an RCA Tablet and the below listed target telephone with associated cellular telephone number of **682-308-1983**, hereinafter referred to as SUBJECT DEVICES, belonging to Grady Bruce Dedmon and Tonia Dedmon, and more particularly described in Attachment A, which is incorporated herein by reference, for the items specified in Attachment B, constituting instrumentalities and evidence of the foregoing violations.

INTRODUCTION

1. I am a Task Force Officer with the Federal Bureau of Investigation ("FBI") and have been so employed since approximately December 2016. I am currently assigned to the Fort Worth, Texas, Division. I have been employed with the Fort Worth Police Department for twenty five years and have been a Detective since 2009. I am currently a Detective assigned to the Fort Worth Police Department Robbery Unit.

Located within the items to be searched, I seek to seize evidence and instrumentalities of criminal violations, which relate to the knowing transportation and possession of child pornography. I request authority to search the SUBJECT DEVICES and other evidence, for the items specified in Attachment B (which is incorporated herein by reference), and to seize and retain all items listed in Attachment B as instrumentalities and evidence of a crime.

2. The information contained in this affidavit is based on my personal knowledge and experience, my own investigation, and information provided by other law enforcement officers and/or agents. Because this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that the portable electronic devices described above were used in committing violations, to include the transportation, receipt, possession, and distribution of child pornography, and these electronic devices contain evidence to include knowledge and identity, fruits, and instrumentalities of 18 U.S.C §§ 2252 and 2252A violations.

SUMMARY OF RELEVANT TECHNOLOGY

3. The term "computer" refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." *See* 18 U.S.C. § 1030(e)(1).

4. A cellular telephone or mobile telephone is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other cellular telephones or traditional "land line" telephones. A cellular telephone usually includes a "call log," which records the telephone number, date, and time of calls made to and from the phone.

5. In addition to enabling voice communications, cellular telephones now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and electronic mail ("e-mail"); taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars. Cellular telephones may also include global positioning system ("GPS") technology for determining the location of the device.

6. These devices, in addition to functioning as a handheld wireless electronic communication device capable of making and receiving telephone calls, can function as an Internet client with e-mail and web browsing capabilities with Wi-Fi and cellular data connectivity.

7. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

8. The term "Internet" is defined as the worldwide network of computers, a noncommercial, self-governing network devoted mostly to communication and research

with roughly 500 million users worldwide. The Internet is not an online service and has no real central hub. It is a collection of tens of thousands of computer networks, online services, and single user components. In order to access the Internet, an individual computer user must use an access provider, such as a university, employer, or commercial internet service provider ("ISP"), which operates a host computer with direct access to the Internet.

9. The term "Web site" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol.

10. The term "Computer system and related peripherals, and computer media" as used in this affidavit refers to tapes, cassettes, cartridges, streaming tape, commercial software and hardware, computer disks, disk drives, monitors, computer printers, modems, tape drives, disk application programs, data disks, system disk operating systems, magnetic media floppy disks, hardware and software operating manuals, tape systems and hard drives and other computer-related operation equipment, digital cameras, scanners, in addition to computer photographs, Graphic Interchange formats and/or photographs, and other visual depictions of such Graphic Interchange formats, including, but not limited to, JPG, GIF, TIF, AVI, and MPEG.

BACKGROUND ON COMPUTERS AND CHILD PORNOGRAPHY

11. Based on my knowledge and training in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed.

12. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage and social networking.

13. Child pornographers can transpose photographic images from a camera into a computer-readable format with a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

14. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution.

15. The Internet affords collectors of child pornography several different venues for obtaining, viewing and trading child pornography in a relatively secure and anonymous fashion.

16. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

17. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer

software, when the computer was sharing files, and some of the files that were uploaded or downloaded.

18. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet. Electronic files downloaded to a hard drive can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensic tools. When a person "deletes" a file on a home computer, the data contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space - for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

19. For a number of reasons, the use of computers has become one of the preferred methods of trafficking in, trading, producing, and collecting child pornography

and other obscene material. Because the distribution of child pornography is illegal, child pornography is not readily available through legitimate domestic businesses; in contrast, child pornography is widely available via computer from individuals who trade such materials on the Internet. Significantly, an individual can utilize a computer in the privacy of his/her own home or office to locate and interact with other individuals offering or seeking such materials. Moreover, he can do so without revealing his true identity. The use of computers thus provides individuals interested in child pornography or obscenity with a sense of privacy and secrecy. Computers also provide such individuals with a convenient method of storing, organizing, and accessing their collections and information concerning others who collect, trade, or distribute such materials.

FACTS ESTABLISHING PROBABLE CAUSE

20. On February 10, 2017, the Bank of Texas located at 1011 Roberts Cut Off Rd in River Oaks, Tarrant County, Texas, was robbed by a white male, hereinafter referred to as robber, that presented a note saying that the robber had a gun and demanded cash. The teller, fearing for her safety, complied with the robber's demands and gave the robber cash.

21. The robber stepped outside the bank with the cash and was apprehended by River Oaks Police.

22. The robber was identified as Grady Bruce Dedmon. Subsequent to Dedmon's arrest, the $1,000 stolen from the bank and an Alcatel One Touch Cell Phone was seized from Dedmon's person.

23. I interviewed Grady Bruce Dedmon who admitted to the bank robbery and advised he called his sister to tell her he was robbing the bank. I obtained written consent from Dedmon to search his Alcatel One Touch cell phone, model A564C, MEID # 27011318512797911 with the number (682)308-1983.

24. Upon review of the contents of Dedmon's phone, I located several images of child pornography on the phone in violation of 18 U.S.C. § 2251.

25. I noted that at least three images were of a minor female child believed to be approximately 8-10 years of age holding a penis or with a penis in the child's mouth. I noted another image of a nude male child possibly 10-12 years of age straddling a nude male adult.

26. I spoke with Tonia Dedmon, Grady Dedmon's sister, and verified that Grady Dedmon had borrowed her RCA Tablet on more than one occasion since Grady's tablet and computer were seized in September of 2016 on an unrelated investigation by the Texas Rangers.

27. I obtained written consent from Tonia Dedmon to take her tablet pending a forensic search and analysis of its contents for any related evidence of child sexual exploitation.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

28. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer

related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (like hard disks, magneto opticals, and others) can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

29. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving

child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

CONCLUSION

30. Based upon the above information, I respectfully submit that there is probable cause to believe that the RCA Tablet and the target phone, more particularly described in Attachment A, that were obtained from Grady Bruce Dedmon and Tonia Dedmon respectively, which are now in the custody of the FBI, are evidence and instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, and that evidence, more particularly described in Attachment B to this affidavit, of those offenses will be found on these devices. Specifically, I submit the SUBJECT DEVICES will contain evidence such as images, e-mails, text messaging conversations, and other communications between **682-308-1983** and others involved in the possession, receipt, distribution, and transportation of child pornography.

31. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of the devices listed in Attachment A and the seizure of the items listed in Attachment B.

Stephanie Phillips

STEPHANIE PHILLIPS
Task Force Officer
Federal Bureau of Investigation

Subscribed and sworn to before me this March 23, 2017, at 10:00 a.m./p.m. in Fort Worth, Texas.

J. Cureton

JEFFREY L. CURETON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A
Description of Items to be Searched

1. One cellular telephone described as follows: a black Alcatel One Touch cellular telephone, model A564C, MEID #27011318512797911, telephone number 682-308-1983, bearing serial number 535D315E ;
2. One RCA tablet described as follows: an RCA tablet with pink backing with charge cord, serial number P3EH1Z1353D5.

These items are currently located at the Federal Bureau of Investigation, Fort Worth Office, 2601 Meacham Blvd, Fort Worth, Texas, 76137.

ATTACHMENT B
LIST OF ITEMS TO BE SEIZED

All records, documents, data, and information in whatever form that constitute evidence, fruits or instrumentalities of violations of 18 U.S.C. §§ 2252 and 2252A, including:

1. Computer(s), computer hardware, computer drives, computer software, computer passwords, that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.

2. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.

3. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

4. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

5. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to whose with an interest in child pornography.

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

7. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.

8. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.

9. Any and all address books, mailing lists, supplier lists, and any and all documents and records, in any format or medium (including, but not limited to e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

10. Any file, information, or record indicating the telephone number 52-5514575821 and/or associated account(s).

11. Any and all correspondence and communications, to include text messaging and voice calls, or other communication medium concerning violations of 18 U.S.C. §§ 2252 and 2252 A from the telephone(s) listed in Attachment A.

12. Any and all photographs, visual depictions, records, documents, files, folders, videos, and materials (in whatever form) of any person under the age of eighteen years old engaging in any sexually explicit conduct as defined in 18 U.S.C. §§ 2252 and 2252A associated on the portable electronic device utilizing; or that has utilized the cellular telephone(s) listed in Attachment A.

13. Any and all files, folders, records, documents, and materials tending to establish the identity of the owner and/or person utilizing cellular telephone number 682-308-1983.

14. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other sexually explicit activities with any persons under the age of eighteen years old contained in the cellular telephones listed in Attachment A.